UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,827	06/29/2001	Cetin K. Koc	245-59280/MDJ	5028

7590 12/16/2004

One World Trade Center
Suite 1600
121 S.W. Salmon Street
Portland, OR 97204

EXAMINER	
ELMORE, JOHN E	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/895,827	KOC ET AL.	
	Examiner	Art Unit	
	John Elmore	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-13,20 and 21* is/are rejected.

7)☐ Claim(s) *2-4 and 14-19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1, 5-13, and 19 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Miyaji (USPN 5,497,423 – published March 5, 1996) in view of Cremona ("Algorithms for Modular Elliptic Curves," Second Edition, Cambridge University Press, 1997).

Regarding independent claim 1, Miyaji discloses a method of generating an elliptic curve comprising:

determining a class polynomial (column 7, line 53, through column 8, line 19).

But Miyaji does not explain selecting a discriminant and constructing an elliptic curve based on the selected discriminant and class polynomial.

However, Cremona teaches a method of generating an elliptic curve comprising:

selecting a discriminant (discriminant selected by providing integer

invariants c_4 and c_6 which define it; see page 63, paragraph 2); and

constructing an elliptic curve based on the selected discriminant and class polynomial (elliptic curve constructed by computing the coefficients a_i according to the conditions of Proposition 3.1.1 and applying them to equation 3.1.1; see page 63, paragraphs 3 and 4, and page 64, paragraph 2)

for the purpose of providing a simpler algorithm to implement and use (page 65, paragraph 2).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the method of Miyaji with the teaching of Cremona to provide a method of generating an elliptic curve comprising:

selecting a discriminant;

determining a class polynomial; and

constructing an elliptic curve based on the selected discriminant and class polynomial. One would be motivated to do so in order to provide a computationally simpler method of generating an elliptic curve.

Regarding dependent claim 5, Miyaji and Cremona teach all the limitations of claim 1, and further teach adjusting an order of the constructed elliptic curve (order adjusted by forming a twist of the elliptic curve; see Cremona, page 62, section 3.1, paragraph 2, and pages 102 and 103, section 3.9). Therefore, for the reasons given above, such a claim would also be obvious.

Regarding dependent claim 6, Miyaji and Cremona teach all the limitations of

claim 5, and further teach a method wherein the order of an elliptic curve is adjusted by forming a twist (see Cremona, page 62, section 3.1, paragraph 2, and pages 102 and 103, section 3.9). Therefore, for the reasons given above, such a claim would also be obvious.

Regarding dependent claim 7, this is a computer-readable medium version of the claimed method steps discussed above (claim 6), wherein all claim limitations have been addressed. Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding dependent claim 8, this is a computer-readable medium version of the claimed method steps discussed above (claim 1), wherein all claim limitations have been addressed. Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding dependent claim 9, Miyaji and Cremona teach all the limitations of claim 1, and further teach

selecting a prime number based on the selected discriminant (list of prime number divisors generated from the discriminant in determining minimal model of elliptic curve per the Kraus-Laska-Connell algorithm; see page 64, section 3.2); and

determining an order of the constructed elliptic curve based on the prime number (order computed by relation of prime number to trace of Frobenius; see Cremona, page 102, section 3.9, paragraph 1).

Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding independent claim 10, Miyaji discloses a cryptographic method comprising requesting construction of an elliptic curve (column 7, lines 6-14), but does not explain providing an elliptic curve based on a selected discriminant.

However, Cremona teaches a method of providing an elliptic curve based on the selected discriminant (elliptic curve provided by computing coefficients a_i according to the conditions of Proposition 3.1.1 and applying them to equation 3.1.1 based on the selection of a discriminant as defined by integer invariants c_4 and c_6; see page 63, paragraphs 2-4, and page 64, paragraph 2) for the purpose of providing a simpler algorithm to implement and use (page 65, paragraph 2).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the method of Miyaji with the teaching of Cremona to provide a method of generating an elliptic curve comprising requesting construction of an elliptic curve and constructing an elliptic curve based on a selected discriminant. One would be motivated to do so in order to provide a computationally simpler method of generating an elliptic curve.

Regarding independent claim 11, this is a computer-readable medium version of the claimed method steps discussed above (claim 10), wherein all claim limitations have been addressed. Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding dependent claim 12, Miyaji and Cremona teach all the limitations of claim 10, and further teach a method comprising obtaining a class polynomial wherein the elliptic curve is based on a root of the class polynomial (see Miyaji, column 7, line

53, through column 8, line 19). Therefore, for the reasons given above, such a claim would also be obvious.

Regarding independent claim 13, this is a cryptographic processor version of the claimed method steps discussed above (claim 10), wherein all claim limitations have been addressed. Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding independent claim 19, this is a computer processor version of the claimed method steps discussed above (claim 10), wherein all claim limitations have been addressed. Therefore, for reasons applied above, such a claim also would have been obvious.

Allowable Subject Matter

3. **Claims 2-4, 14-18, 20 and 21 are objected to as being dependent upon a rejected base claim, but would be allowable** if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Regarding dependent claim 2, the closest prior art, Miyaji and Cremona, teach all the limitations of claim 1, but Miyaji and Cremona do not explain a method comprising storing a set of discriminants and selecting a determinant from the stored set. The prior art teaches the method wherein only one elliptic curve is generated at a

time: a determinant is provided, the associated curve is evaluated and, if not suitable, then another discriminant is provided. But the prior art does not teach a method wherein a set of discriminants is first constructed before one of the discriminants is selected from the set for evaluation as a suitable curve. Therefore, claim 2 is allowable.

Regarding dependent claim 3, the closest prior art, Miyaji and Cremona, teach all the limitations of claim 2, but Miyaji and Cremona do not explain a method comprising storing a set of class polynomials and obtaining the selected class polynomial from the set of class polynomials. The prior art teaches the method wherein only one elliptic curve is generated at a time; the class polynomial determinant is provided (derived from the discriminant), the associated curve is evaluated, and if not suitable, then another class polynomial is provided. But the prior art does not teach a method wherein a set of class polynomials is first constructed before one of the class polynomials is selected from the set for evaluation as a suitable curve. Therefore, claim 3 is allowable.

Dependent claim 4 is allowable for the same reasons as provided above in claim 3.

Dependent claim 14 is allowable for the same reasons as provided above in claim 2.

Dependent claim 15 is allowable for the same reasons as provided above in claim 3.

Dependent claim 16 is allowable for the same reasons as provided above in claim 3.

Dependent claim 17 is allowable for the same reasons as provided above in claim 3.

Dependent claim 18 is allowable for the same reasons as provided above in claim 2.

Dependent claim 20 is allowable for the same reasons as provided above in claim 2.

Dependent claim 21 is allowable for the same reasons as provided above in claim 2.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).